

Identification du service G-Cloud

ShaD – Shared Directory

Description du service G-Cloud

ShaD est la solution centrale de gestion des identités pour les services G-Cloud. ShaD permet aux utilisateurs de différentes institutions gouvernementales de se connecter aux applications G-Cloud avec leurs informations d'identification existantes. Et ceci tout en conservant la propriété de son propre répertoire d'identités local.

ShaD est basé sur les principes suivants:

- Authentification simplifiée des utilisateurs de différentes institutions.
- Centralisation des applications communes basée sur l'identification avec l'AD de chaque institution.
- Maintien de la gestion des comptes d'utilisateurs dans chaque institution.
- Impact minimal sur les AD existantes des institutions.

Différents modèles d'authentification sont pris en charge en fonction du type d'application:

1. Services de fédération ShaD

Prend en charge l'authentification unique dans les applications « claims-aware ». Ce service est basé sur une fédération SAML reposant sur un serveur ADFS géré par ShaD.

1. *ShaD Online Services*

Fournit la connectivité à Azure AD et l'identification de l'utilisateur à Office 365. Active les fonctionnalités hybrides dans UCCaaS, fonctionnalités grâce auxquelles les services peuvent être utilisés de manière transparente entre UCCaaS et Office 365.

Ce service est basé sur les mêmes fondements que la fédération ShaD au niveau des institutions.

Il existe une couche de synchronisation des AD d'une institution vers Azure AD (Office 365) via Azure AD Connect. Ces services sont gérés par ShaD et doivent être centralisés pour G-Cloud Azure AD.

Composants

Active Directory Federation Services (ShaD-FS)

ShaD maintient une infrastructure ADFS avec haute disponibilité. Cette infrastructure offre une authentification via le protocole SAML. Ce service nécessite un serveur SAML fonctionnel dans l'institution (accessible uniquement aux utilisateurs).

L'équipe ShaD peut fournir un soutien et des conseils pour l'organisation et l'utilisation du système ADFS du côté de l'institution, mais n'assume aucune responsabilité quant à sa disponibilité.

Azure AD Connect (ShaD-Online)

ShaD maintient une configuration redondante d'Azure AD Connect. Ce service synchronise les informations nécessaires de AD de l'institution avec Azure AD (uniquement les attributs nécessaires, pas de mots de passe).

La synchronisation normale, également appelée synchronisation Delta, ne traite que les différences et est traitée dans l'heure. Dans certaines situations, telles qu'une mise à niveau ou un changement vers un AD de l'institution, une synchronisation complète est requise. Une telle resynchronisation complète est initiée par ShaD et nécessite jusqu'à 24 heures.

Responsable du service

FPD – Luc Coppens – shad@gcloud.belgium.be

Niveaux de service

- Disponibilité ShaD FS: 99% (24/7)
- Azure AD Connect Delta Synchronisation: 1x par heure, 8h/jour, 5j/semaine (synchronisation complète 1x / jour)

Coûts

L'utilisation de l'infrastructure ShaD n'est pas sujette à des coûts.

Quelles sont les évolutions possibles ?

Le service ShaD suivra les évolutions technologiques et les besoins du G-Cloud.

Evolutions possibles:

- Utilisation de FAS CSAM pour l'authentification
- Interaction simplifiée pour les utilisateurs externes à ShaD

Informations Pratiques



ShaD-Online requiert un certain nombre de services de l'infrastructure AD et réseau d'une institution (propres contrôleurs AD sur un réseau spécifique).

Information et question(s): shad@gcloud.belgium.be